Application No. 10/649,459

EXAMINER INTERVIEW SUMMARY

Applicant and its undersigned representative thank the Examiner for the courtesy extended during the telephonic interview of December 5, 2007. During the interview, claims 1 and 8 were discussed in view of the prior art of record, particularly, Gunsch, Losey et al., and Walter. Applicant's representative advanced arguments that are substantially reflected in the Remarks section of this Amendment. The Interview Summary entered by the Examiner (Paper No. 20071205) is an accurate summary of the substance of the interview. As indicated therein, agreement was reached that the claims are allowable over the prior art of record.

REMARKS

Prior to this Amendment, claims 1-11 were pending. By this Amendment, dependent claims 16-19 are added. Support for the new claims may be found in the Specification in the paragraphs beginning on page 15, line 17, and on page 17, line 33. Claims 1-11 and 16-19 are now pending, and are presented for reconsideration and allowance..

Claim Rejections – 35 U.S.C. § 103

Claims 1-7 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Gunsch (U.S. Publication No. 2003/0117261), in view of Losey et al. (EP1101670), and in further view of Walter (U.S. Pat. No. 6,275,141). Claims 8-11 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Gunsch in view of Losey et al., in view of Walter, and in further view of Murakami et al. (U.S. Patent No. 6,281,599). These rejections are respectfully traversed.

The Gunsch publication

Gunsch discloses configuring a wireless key fob to recognize users using fingerprint readings and providing different levels of access for each user. Different vehicle functions, such as lock/unlock, and trunk access, for example, can be configured in the key fob specific to each user. In Gunsch, when a user attempts to perform an operation, the universal transmitter checks the user's identification using the fingerprint scanner, and determines whether that user is authorized to perform the attempted operation. If the user is not authorized, the universal transmitter simply does not transmit the requested command. See, e.g., Fig. 7B of Gunsch. The

valet mode in Gunsch involves *overriding* the authentication means to provide temporary access to users that have not been pre-authorized.

In contrast to the device disclosed in Gunsch, the electronic key in claims 1 and 8 includes a restriction information generation device that generates specific code corresponding to the operation restriction information registered in the electronic key, and the electronic key wirelessly outputs the specific code corresponding to the operation restriction information registered in the electronic key regardless of what person is carrying the electronic key.

Gunsch is relied upon in the rejections of claims 1 and 8 for teaching, *inter alia*, the use of transmitter 45 to transmit specific codes corresponding to the operation restriction information and the electronic key wirelessly outputs the code. Paragraphs 0065-0067 of Gunsch are cited for this proposition. In fact, those paragraphs relate instead to universality features of the universal transmitter that permit the universal transmitter to work with different vehicles. The "signal codes" referred to in paragraphs 0065-0067 are the codes for simply communicating with different remote keyless entry systems for the different vehicles.

The universal transmitter of Gunsch implements the varying levels of authorization by *abstaining from* transmitting commands that are not authorized. In claims 1 and 8, the specific code itself, and not merely the outputting of any specific code or signal, is what corresponds to the operation restriction information registered in the electronic key. Therefore, Gunsch does not describe outputting the specific code *that corresponds to the operation restriction information registered in the electronic key* regardless of what person is carrying the electronic key, as claimed in claims 1 and 8.

The Office Action has acknowledged that Gunsch does not describe a control unit to perform wireless communication or the generation of restriction information for wireless transmission. The Office Action further acknowledges that Gunsch lacks the teaching of a restriction control device with a second verification device arranged within the vehicle.

The Losey et al. publication

Losey et al. discusses a vehicle-based controller in which different levels of security, such as access to accessories, can be configured via an interface. The controller responds to different authorization codes according to the *controller's* configuration. Authorization codes are transmitted by signaling devices, and a signaling device can selectively provide more than one authorization code. The Losey et al. system permits security to be configured in the vehicle-based controller, and is relied upon in the Office Action essentially for teaching different levels of security provided by the vehicle-based controller in response to wireless communication.

The selectable authorization code output by the signaling device may correspond to certain known access permissions, but these access permissions are defined in the vehicle-based controller, and not in the signaling device. The Office Action acknowledges that Losey et al. also fails to teach generation of specific restriction information for wireless transmission, as claimed in claims 1 and 8.

Therefore, Losey et al. also fails to describe a restriction information generation device *in the electronic key* that generates restriction information for wireless transmission, as claimed in claims 1 and 8. Instead, Losey et al. discloses configuring the vehicle-based controller to

respond to different transmitted authorization codes, without any teaching of transmission of restriction information from the signaling device to the controller.

The Walter patent

The Walter patent describes a vehicle restricted access valet mode system. Various embodiments discussed in the Walter patent disclose a remote control device that can be used to toggle between full access, or restricted access to the vehicle. However, Walter is silent as to registering restriction information in an electronic key, and outputting a specific code *corresponding to operation restriction information registered in the electronic key*, a as claimed in claims 1 and 8.

In Walter, instead of registering restriction information in the electronic key as in the present invention, the restricted access valet mode/normal mode can simply be remotely selected by either connecting or disconnecting a connector, key, key ring, or ID tag, from the remote control (*see* col. 3, line 32, *et seq.*). In another embodiment, the remote control can be physically separated into two parts, and transmit either a first signal or a second signal (indicating the access mode) depending on whether the two parts are connected or disconnected (*see* col. 3, line 53, *et seq.*). In another embodiment disclosed by Walter, the restricted access mode may be selected via the remote control by entering a certain code, such as pressing the "open fuel door" button a predetermined number of times in a certain time interval (*see* col. 20, line 36 *et seq.*). The signals transmitted by the remote control go to a processing unit located in the vehicle, and the processing unit in turn activates or deactivates the restricted access valet mode (*see* col. 9, line 31 *et seq.*).

Walter also discloses a remote control having various buttons for independently controlling different systems of the vehicle, such as opening the trunk, opening, the door, or opening the fuel door (see col. 10, line 1, *et seq.*). These functions are not related to *registering* restriction information *in the electronic key*, or outputting a specific code corresponding to the restriction information registered in the electronic key, as claimed in claims 1 and 8.

The Walter patent further discloses customizing the restricted access mode by manipulating controls located in the car, such as the on the car's radio. This portion of Walter's disclosure is cited in the Office Action and relied upon for teaching that the remote may transmit signals even when the system is placed in a restricted state. Applicant respectfully points out that the signals referred to in Col. 22, lines 35-40 of Walter are signals from the vehicle's radio 534 to the vehicle's processing unit 116, and not from the remote device to the vehicle. Applicant cannot find in Walter any enabling description of customizing the restricted access mode in the processing unit by operation of the remote. Moreover, even assuming *arguendo* that there were a teaching of remote customization of a vehicle controller or processing unit for different restriction settings, that disclosure would still fail to destroy patentability of the claimed limitation of outputting, by the electronic key, a specific code *corresponding to operation restriction information registered in the electronic key*, as claimed in claims 1 and 8.

Gunsch, Losey et al., Walter, and Murakami et al. cannot be combined to achieve the claimed invention

Among the references relied upon in the § 103 rejection of claims 1 and 8, there is no teaching or suggestion of registration of operation restriction information in the electronic key,

and of the electronic key wirelessly outputting the specific code corresponding to the operation restriction information registered therein regardless of what person is carrying the electronic key, as claimed.

Gunsch does not recognize selectively limiting vehicle access for valets. In the valet mode of Gunsch, the user authorization functionality is overridden. The universal transmitter of Gunsch apparently only permits limiting access to the vehicle for registered users. The systems of Losey et al. and Walter would permit the vehicle-based controller to be selectively configured into a restricted access mode, but do not provide any description of doing so remotely, let alone registering the restriction information in an electronic key as in claims 1 and 8. Thus, one of the benefits offered by the claimed invention–that is, being able to configure an electronic key for particularized restricted access to the vehicle, doing so remotely from the vehicle (and even outside communications range of the vehicle), and without having to pre-register a user for restricted access–is not available by any system or functionality achievable by combining Gunsch, Losey et al, Walter, and Murakami.

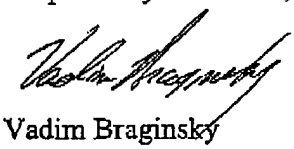
In view of the above, not all elements present in either of claim 1 or claim 8 are taught or suggested by any combination of Gunsch, Losey et al., Walter, and Murakami. Therefore, a *prima facie* case for obviousness has not been made, and cannot be maintained with respect to claims 1 and 8 on the basis of these references. Since each of dependent claims 2-7, 9-11, and 16-19 further limits its respective base claim, these claims are also believed to be allowable. Withdrawal of the § 103 rejections is respectfully requested.

Conclusion

In view of the foregoing, it is submitted that this application is in condition for allowance. Favorable consideration and prompt allowance of the application are respectfully requested.

The Examiner is invited to telephone the undersigned if the Examiner believes it would be useful to advance prosecution.

Respectfully submitted,



Vadim Braginsky
Registration No. 58,031

Customer No. 24113
Patterson, Thuente, Skaar & Christensen, P.A.
4800 IDS Center
80 South 8th Street
Minneapolis, Minnesota 55402-2100
Telephone: (612) 252-1542